The Doxing Bible

Religion of Web Forensics

Created by Dubitus and Ego of The Black Hand

Contents

Introduction

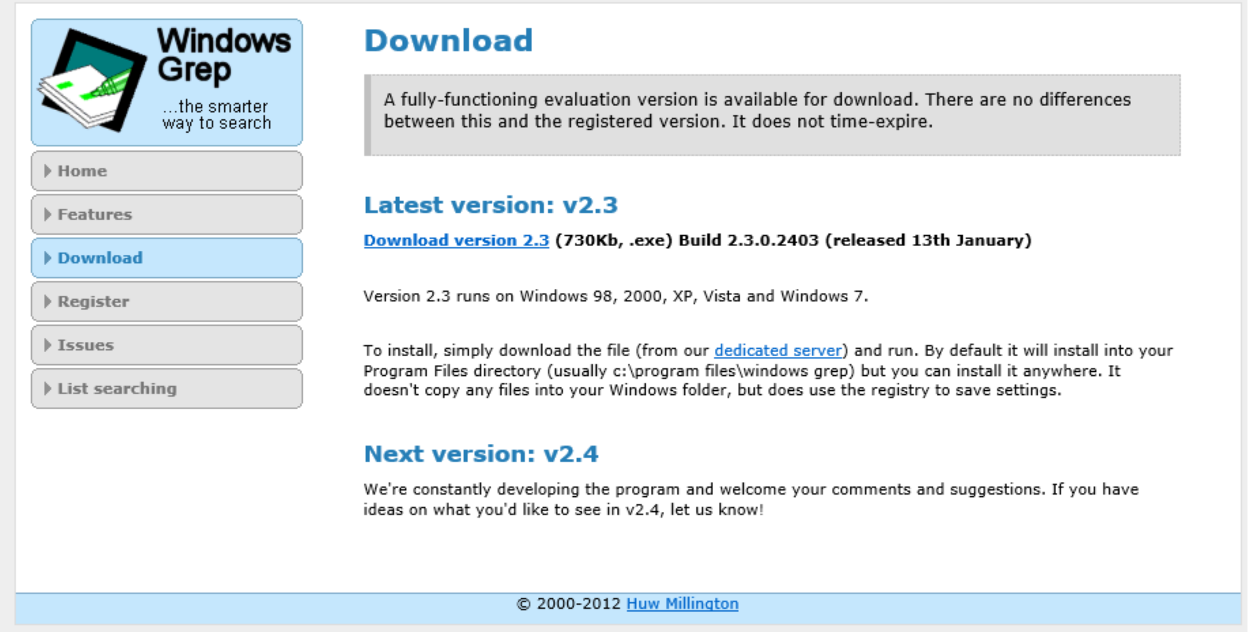
Welcome to the official online resource known as "*The Doxing Bible*", you have now officially placed yourself in a position to gain far more knowledge than the common forensic investigator and we are glad you chose wisely with your resources. This eBook will not only allow you to implement theory into practical work, but you will have your own forensic service up and running in no time. The resource has been compiled and compressed into a single booklet that will teach you the key aspects of web forensics investigating (*doxing*), and web forensics removal (*footprint removal*), both of which have been created and published by two experienced web forensic investigators who established a presence on forums. Throughout the years, there have been many forensic related services and eBooks that allow you to somewhat get a grasp of what doxing is and how it can contribute or be somewhat beneficial, however these eBooks would only contribute/inform you about a small portion of the whole forensic framework, which both Dubitus and myself deemed extremely repetitive and saturated. This is why we are offering the "*Bible*" of all doxing ebooks and we are even adding private methods to increase it's value and to ensure that it is unsaturated. So, without further adieu, allow us to indulge you in the best forensic ebook on the market, the book that is known as "*The Doxing Bible*".

Chapter One

1.1 - Computer Forensics: Database Forensics - GREP

Windows GREP is a simple tool that will help you by searching files for text strings that you specify (*in this case, databases*). There are many other file searching programs, but Windows GREP is the most versatile and is very user-friendly.

We'll be using it to browse strings containing information on publicly obtainable database dumps. We want usernames, emails, IPs, date of birth, anything personal from those databases when we search for a specific term.
You start by going to their download page here: http://www.wingrep.com/download.htm and download the latest version of it.



Download

A fully-functioning evaluation version is available for download. There are no differences between this and the registered version. It does not time-expire.

Latest version: v2.3

Download version 2.3 (730Kb, .exe) Build 2.3.0.2403 (released 13th January)

Version 2.3 runs on Windows 98, 2000, XP, Vista and Windows 7.

To install, simply download the file (from our dedicated server) and run. By default it will install into your Program Files directory (usually c:\program files\windows grep) but you can install it anywhere. It doesn't copy any files into your Windows folder, but does use the registry to save settings.

Next version: v2.4

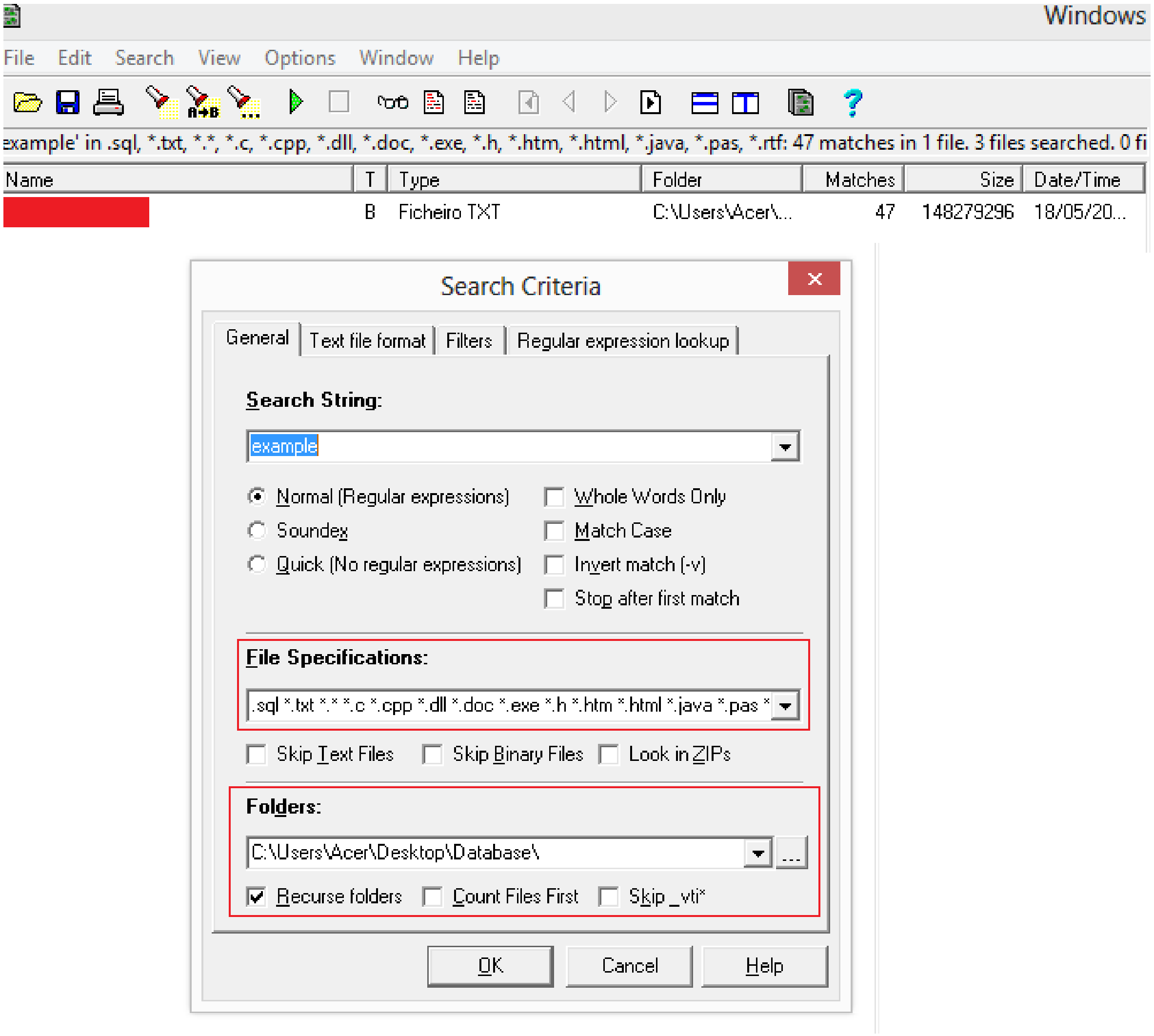
We're constantly developing the program and welcome your comments and suggestions. If you have ideas on what you'd like to see in v2.4, let us know!

© 2000-2012 Huw Millington

After you've downloaded it, you need to create a folder on your desktop called "*Database*" and then you install Windows GREP and set it up properly by giving it a directory (*C:/user/XXX/desktop/database*) and specific files to search for (*.sql *.txt *.* *.c *.cpp *.dll *.doc *.exe *.h *.htm *.html *.java *.pas *.rtf*).

You really need to establish a path to GREP (*Database*) and your really need to specify the file types so that GREP can work properly.

After you've created the folder, installed GREP and put in all the file types, it will look something like this:


Windows
File Edit Search View Options Window Help
Search Criteria
General
Text file format
Filters
Regular expression lookup
OK
Cancel
Help

xample' in .sql, *.txt, *.*, *.c, *.cpp, *.dll, *.doc, *.exe, *.h, *.htm, *.html, *.java, *.pas, *.rtf: 47 matches in 1 file. 3 files searched. 0 fi

Name	T	Type	Folder	Matches	Size	Date/Time
[redacted]	B	Ficheiro TXT	C:\Users\Acer\...	47	148279296	18/05/20...

Search String:

example

● Normal (Regular expressions) ○ Soundex ○ Quick (No regular expressions)

□ Whole Words Only □ Match Case □ Invert match (-v) □ Stop after first match

File Specifications:

.sql *.txt *.* *.c *.cpp *.dll *.doc *.exe *.h *.htm *.html *.java *.pas *

□ Skip Text Files □ Skip Binary Files □ Look in ZIPs

Folders:

C:\Users\Acer\Desktop\Database\

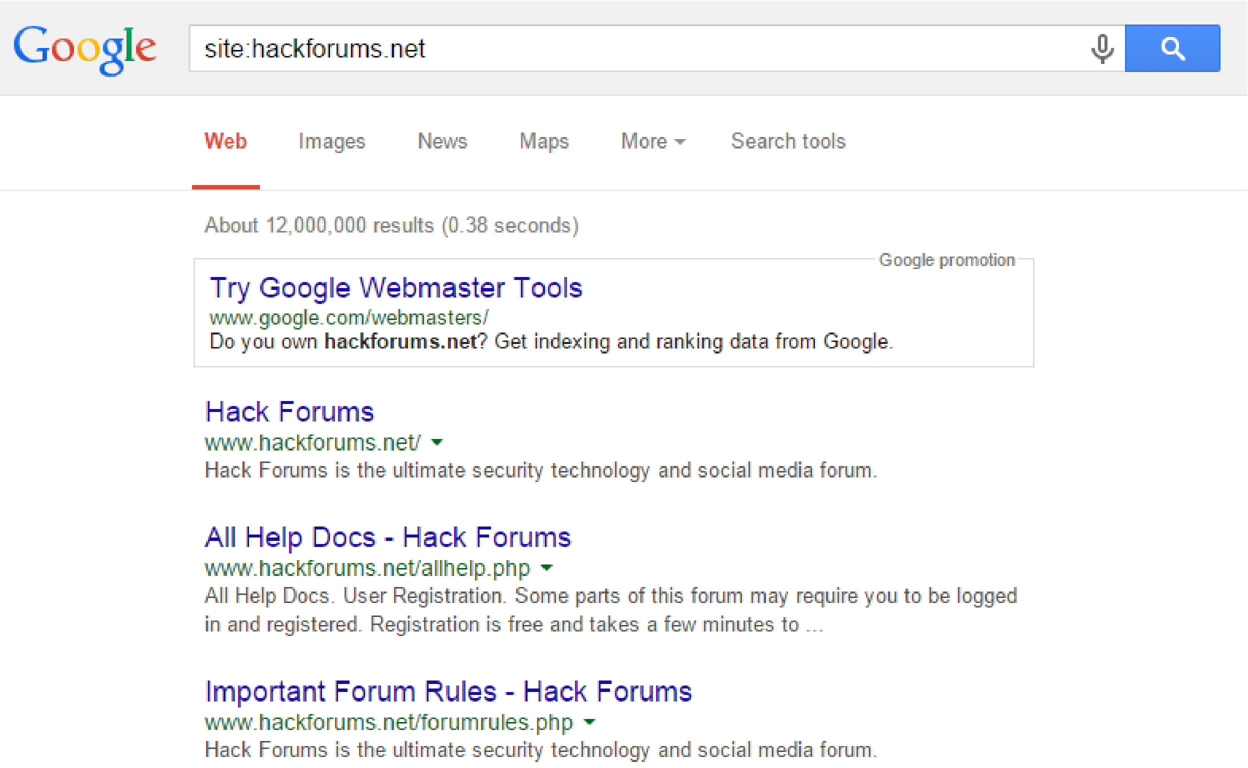
☑ Recurse folders □ Count Files First □ Skip _vti*

After you have everything setup, you can start growing your folder by adding new databases to it. You can search on multiple hacking forums for database dumps, or you can search the entire web by running this search operator: filetype:sql "username , password" (*copy exact sentence*).

1.2.1 Web & Network Forensics: Google Search Operators

Google Search Operators will be your bread and butter when doing web forensics. They help you by filtering out information so that you can work your resources more efficiently and with more accuracy. Without the operator's you would be stuck with thousands and thousands of pages.

The first thing you need to work with the operators: the place (*of the target*). if your target is on a website, you start by filtering the search by using the operator "***site:***". In this case, lets use the famous website hackforums.net.



About 12,000,000 results (0.38 seconds)

Google promotion

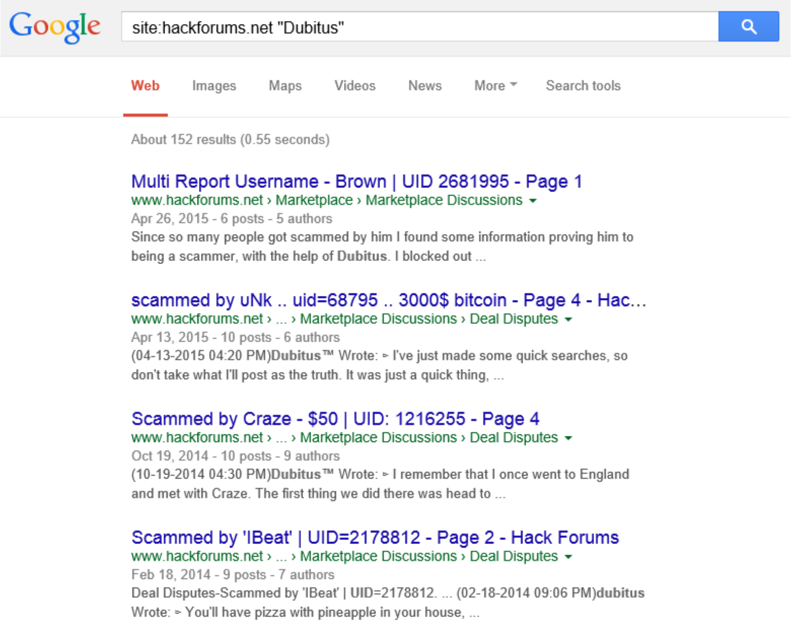
Try Google Webmaster Tools
www.google.com/webmasters/
Do you own **hackforums.net**? Get indexing and ranking data from Google.

Hack Forums
www.hackforums.net/
Hack Forums is the ultimate security technology and social media forum.

All Help Docs - Hack Forums
www.hackforums.net/allhelp.php
All Help Docs. User Registration. Some parts of this forum may require you to be logged in and registered. Registration is free and takes a few minutes to ...

Important Forum Rules - Hack Forums
www.hackforums.net/forumrules.php
Hack Forums is the ultimate security technology and social media forum.

Now that we have a place to work with, we need a target. To narrow a term that you're looking for, you use the quotation marks "**term**". Lets use myself "**dubitus**" as the target.



site:hackforums.net "Dubitus"

About 152 results (0.55 seconds)

Multi Report Username - Brown | UID 2681995 - Page 1
www.hackforums.net › Marketplace › Marketplace Discussions
Apr 26, 2015 - 6 posts - 5 authors
Since so many people got scammed by him I found some information proving him to being a scammer, with the help of **Dubitus**. I blocked out ...

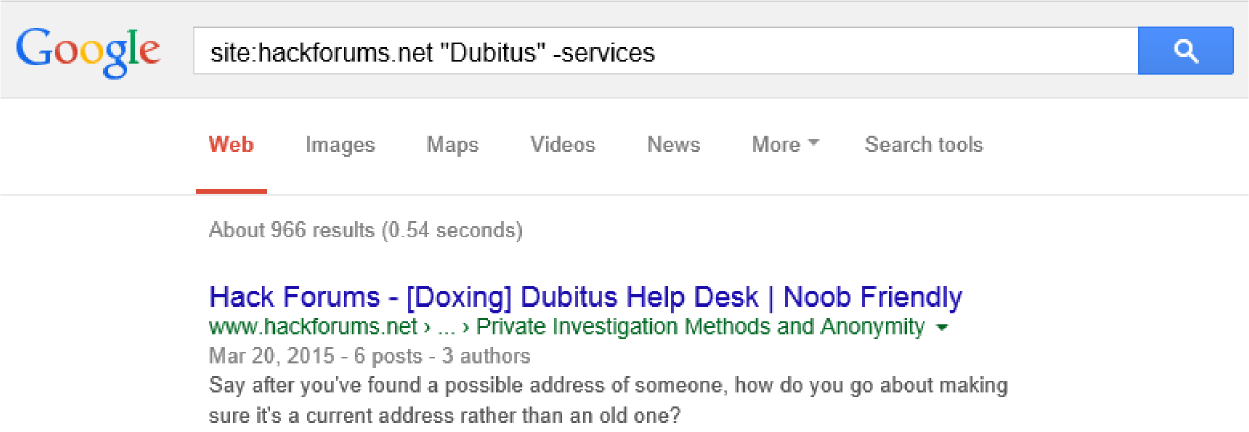
scammed by uNk .. uid=68795 .. 3000$ bitcoin - Page 4 - Hac...
www.hackforums.net › ... › Marketplace Discussions › Deal Disputes
Apr 13, 2015 - 10 posts - 6 authors
(04-13-2015 04:20 PM)**Dubitus**™ Wrote: ▸ I've just made some quick searches, so don't take what I'll post as the truth. It was just a quick thing, ...

Scammed by Craze - $50 | UID: 1216255 - Page 4
www.hackforums.net › ... › Marketplace Discussions › Deal Disputes
Oct 19, 2014 - 10 posts - 9 authors
(10-19-2014 04:30 PM)**Dubitus**™ Wrote: ▸ I remember that I once went to England and met with Craze. The first thing we did there was head to ...

Scammed by 'IBeat' | UID=2178812 - Page 2 - Hack Forums
www.hackforums.net › ... › Marketplace Discussions › Deal Disputes
Feb 18, 2014 - 9 posts - 7 authors
Deal Disputes-Scammed by 'IBeat' | UID=2178812. ... (02-18-2014 09:06 PM)**dubitus** Wrote: ▸ You'll have pizza with pineapple in your house, ...

As you can see, it narrows down the search results to pretty much anything I posted or that was posted regarding the term “**Dubitus**” on “**site:hackforums.net**”.

Now lets say we wanted to remove the results that contain “**services**”, because we’re not interested in that term. What we do is, we add the minus “**-**” operator to the term, like this “**-services**”.



site:hackforums.net "Dubitus" -services

About 966 results (0.54 seconds)

Hack Forums - [Doxing] Dubitus Help Desk | Noob Friendly
www.hackforums.net › ... › Private Investigation Methods and Anonymity
Mar 20, 2015 - 6 posts - 3 authors
Say after you've found a possible address of someone, how do you go about making sure it's a current address rather than an old one?

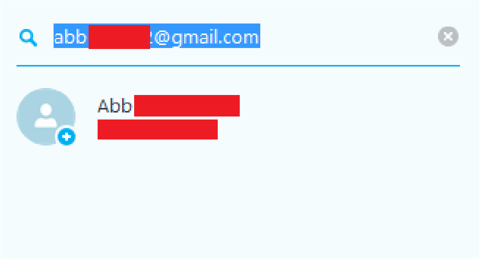
Those are the 3 more important operators that you will work with. You can also use the “**cache:**” operator to check for posts that have been deleted, but are still indexed on the search engine.

Now this is when you start being creative. You can use terms like **site:hackforums.net “dubitus” “skype”** or something like **site:hackforums.net “dubitus” “contact”** or **site:hackforums.net “dubitus” “@gmail.com”** , that will help you find personal information on the target if it was posted, like skype, contact details or emails.

For more information regarding the google operators, please visit: https://support.google.com/websearch/answer/2466433?hl=en&rd=1

1.2.2 Web & Network Forensics: Skype Email Resolver

This is where you're going to learn how to search for a skype by using an email. Whenever you find an email, always check if it has a skype associated with it by going to the skype search.

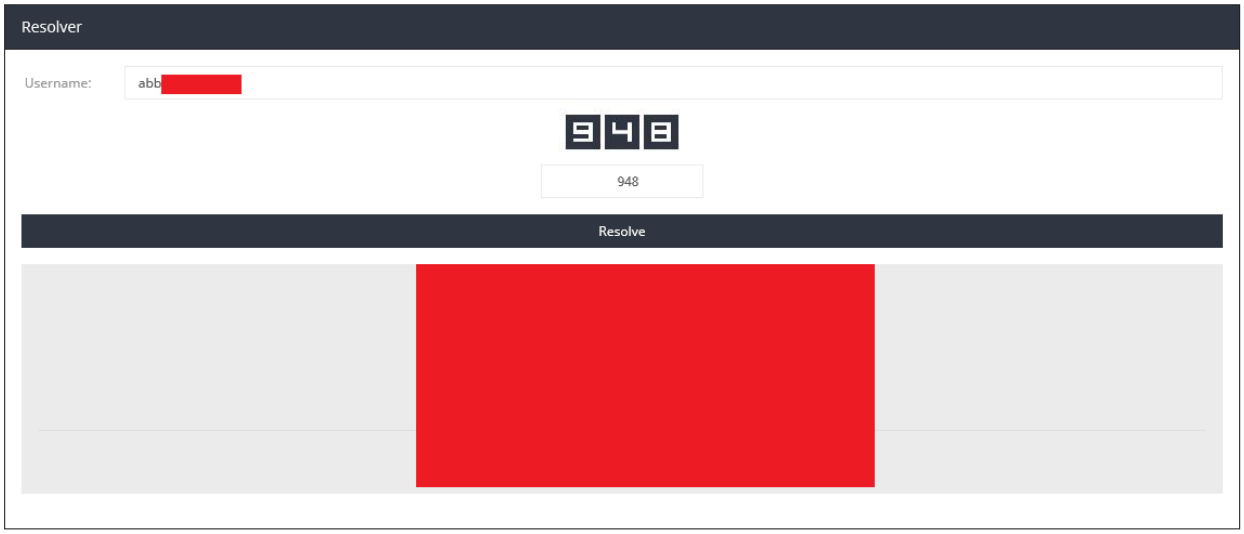


abb[redacted]@gmail.com

Abb[redacted]

[redacted]

This way you'll find the person's skype from the email associated. Then you can resolve the skype to actually get the IP from any skype resolver, like this one: skypegrab.net/



Resolver

Username: abb[redacted]

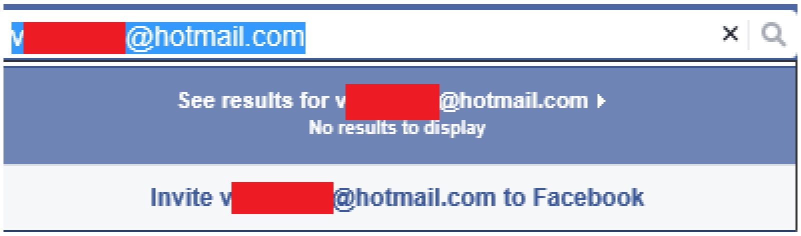
948

[redacted]

You can also do IP-to-Skype on that skype resolver to find associated skypes with the IP.

1.2.3 Web & Network Forensics: Facebook Hidden Email & Phone Resolver

Sometimes when you search for a Facebook profile using the email or phone number, nothing will pop up. That's because it's not associated with any profile, or the person has made the privacy settings hidden (*email and phone*) from the facebook search.



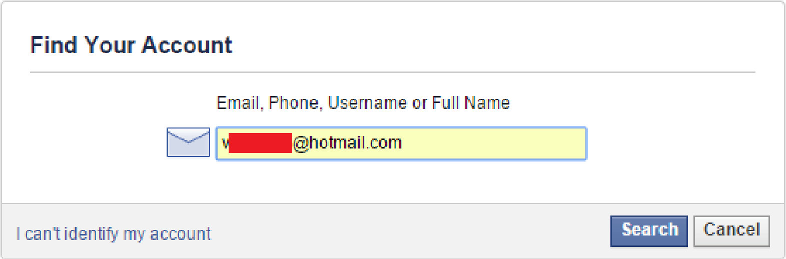
v[redacted]@hotmail.com

See results for v[redacted]@hotmail.com

No results to display

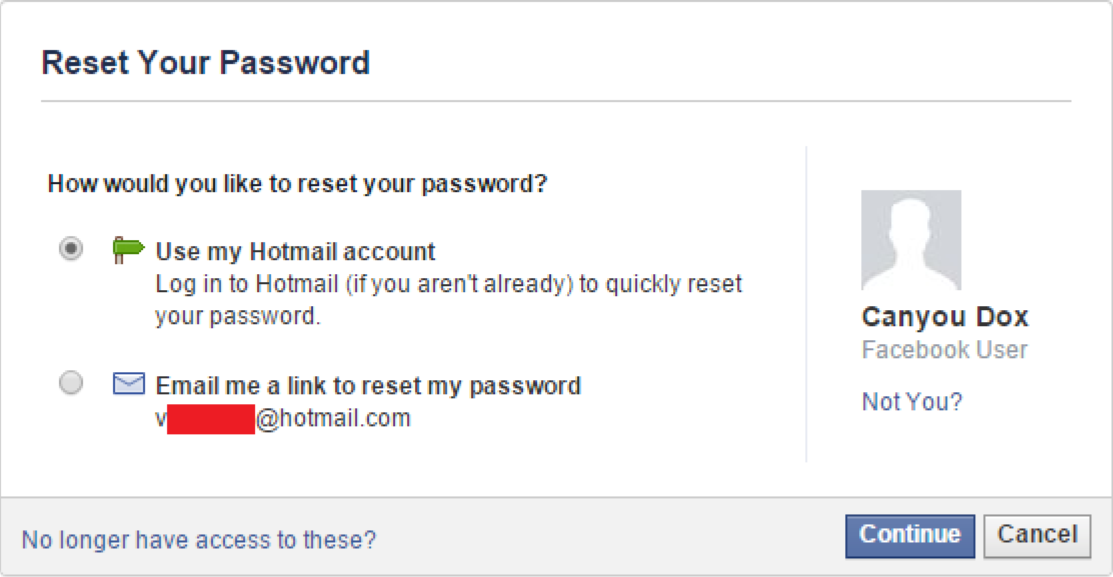
Invite v[redacted]@hotmail.com to Facebook

So what you do to bypass this security aspect is a simple trick. You go to the forgot password of Facebook, and try looking there.



Find Your Account

Email, Phone, Username or Full Name: v[redacted]@hotmail.com



Reset Your Password

How would you like to reset your password?

● Use my Hotmail account
Log in to Hotmail (if you aren't already) to quickly reset your password.

○ Email me a link to reset my password
v[redacted]@hotmail.com

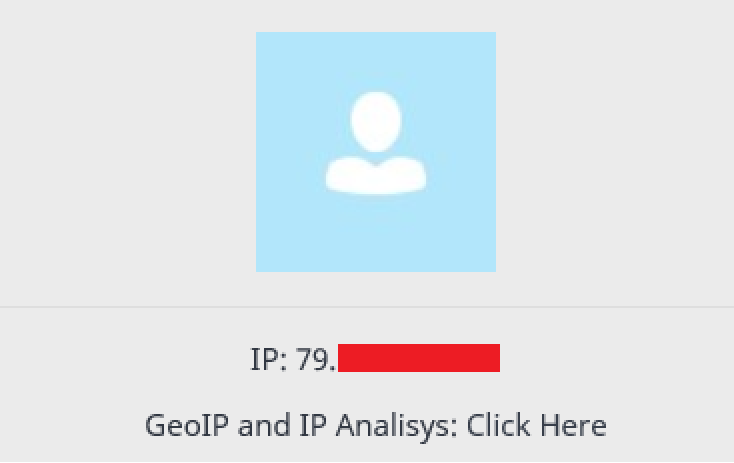
Canyou Dox
Facebook User

And this is how you bypass the hidden feature on Facebook for emails and phone numbers.

1.2.4 Web & Network Forensics: IP Location Analysis & Resolver

This topic will help you narrow down the location of your target. It can also help you identify if your target is using a proxy.

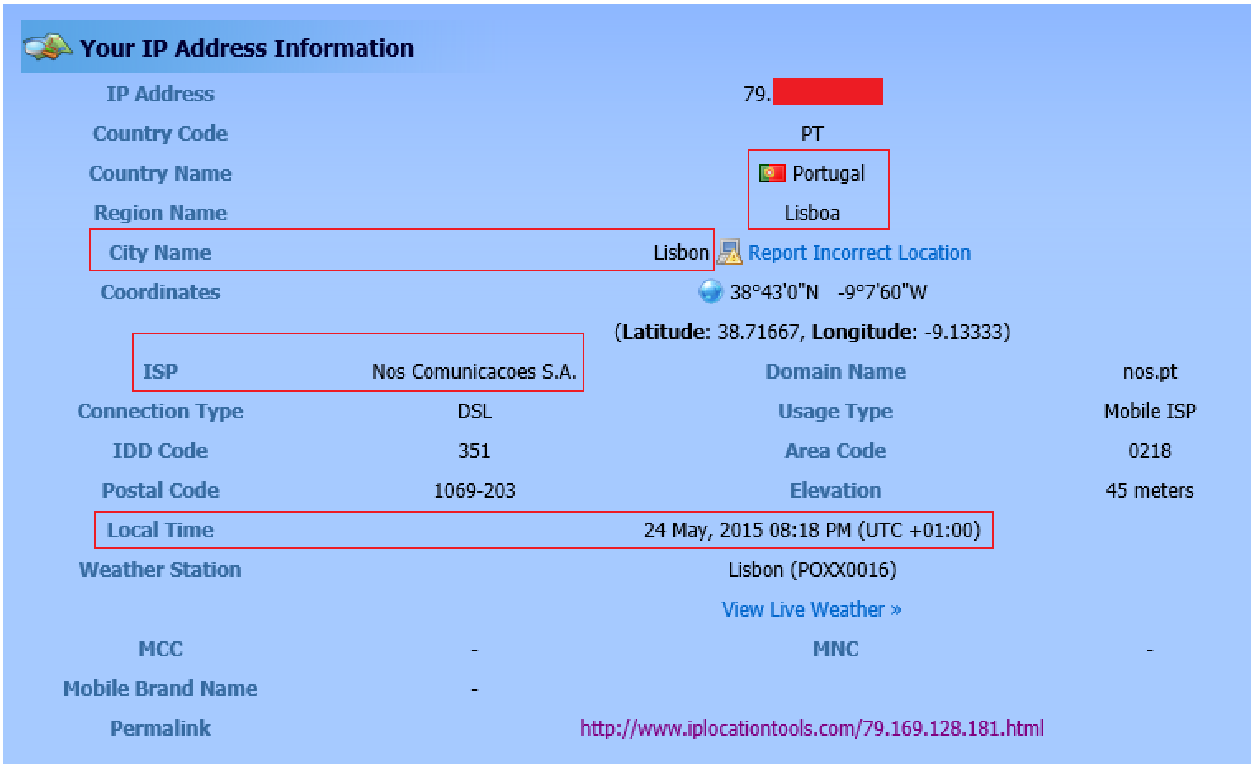
Once you find the IP from resolving a skype, you want to make sure you narrow down the location. Lets try my skype as an example (you can use skypegrab.net/).



IP: 79.[redacted]

GeoIP and IP Analisys: Click Here

Now that you have the IP, you go to this website and insert the IP next to the URL: http://www.iplocationtools.com/79.XXX.XXX.XXX.html and you'll get something like this.

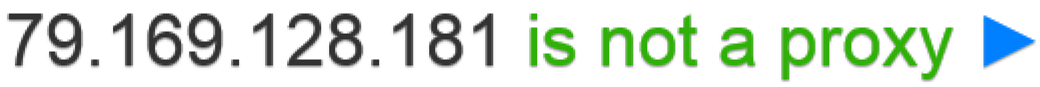


Your IP Address Information

IP Address	79.[redacted]		
Country Code	PT		
Country Name	Portugal		
Region Name	Lisboa		
City Name	Lisbon Report Incorrect Location		
Coordinates	38°43'0"N -9°7'60"W (**Latitude:** 38.71667, **Longitude:** -9.13333)		
ISP	Nos Comunicacoes S.A.	Domain Name	nos.pt
Connection Type	DSL	Usage Type	Mobile ISP
IDD Code	351	Area Code	0218
Postal Code	1069-203	Elevation	45 meters
Local Time	24 May, 2015 08:18 PM (UTC +01:00)		
Weather Station	Lisbon (POXX0016) View Live Weather »		
MCC	-	MNC	-
Mobile Brand Name	-		
Permalink	http://www.iplocationtools.com/79.169.128.181.html		

As you can see, you can determinate that I'm from Lisbon, Portugal and my ISP (Internet Service Provider) is Nos Comunicacoes S.A., which means it's a legitimate IP. That will help you to narrow down locations.

To find out if it's a proxy, you can visit http://www.proxyornot.com/ and it will retrieve the result based on the IP.

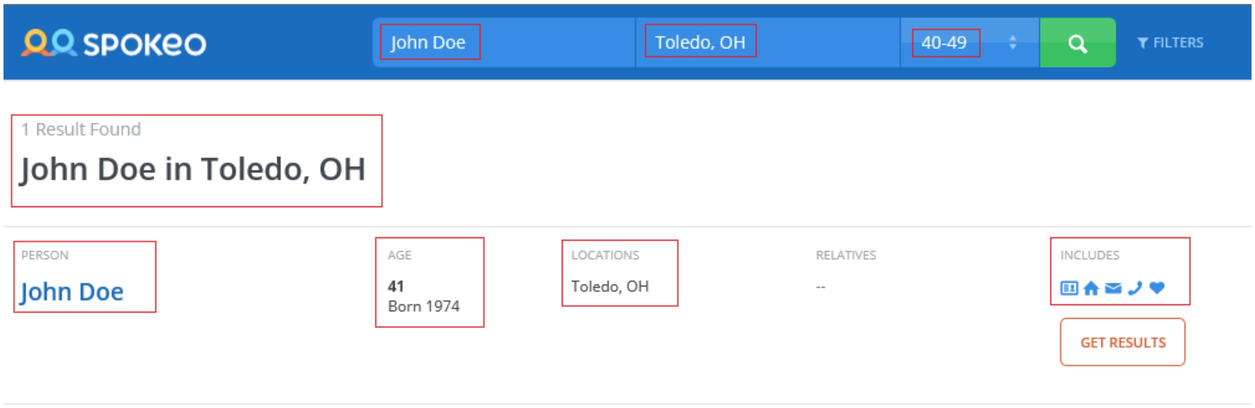

79.169.128.181 is not a proxy ▶

1.2.5 Web & Network Forensics: People Search Directories

A People Search Directory is a free or paid service that allows you to search people by name or phone number and find out who owns it using reverse phone lookup or public records.

So lets say that we know that our target is named **John Doe** and according to the **IP** we resolved from the Skype we got his location which was **Toledo, Ohio** and from that same Skype lets assume he stated his Year of Birth (**1947**) and age (**41**).

We would go to a a People Search Directory, which we can use a very common called spokeo.com .



John Doe | Toledo, OH | 40-49

1 Result Found

John Doe in Toledo, OH

PERSON	AGE	LOCATIONS	RELATIVES	INCLUDES
John Doe	41 Born 1974	Toledo, OH	--	

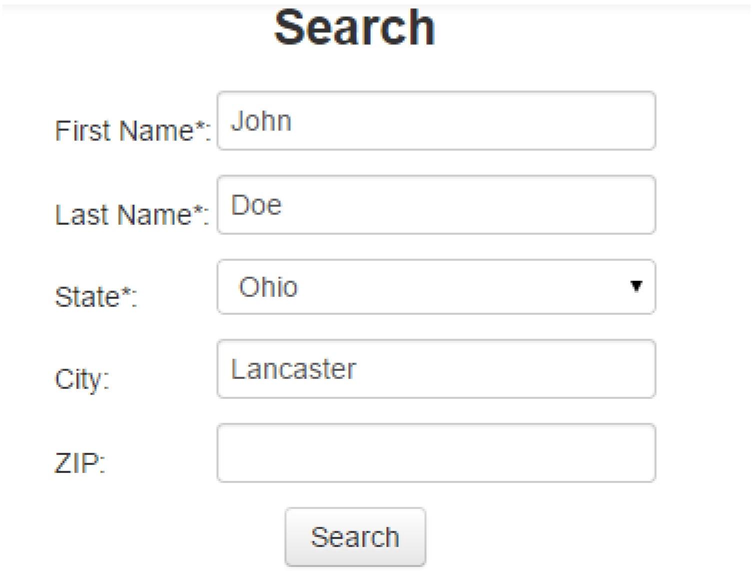
From there you will find his whole information by just clicking in **John Doe**. Please remember that Spokeo is a paid service.

You can alternatively go to the white-pages for free results, here: whitepages.com

1.2.6 Web & Network Forensics: SSN Lookup (*USA/UK*)

There is the option to look for the **SSN** (**Social Security Number**) of your target if he's from the **USA** or **UK**. The website that sells that kind of information is https://ssndob.so .

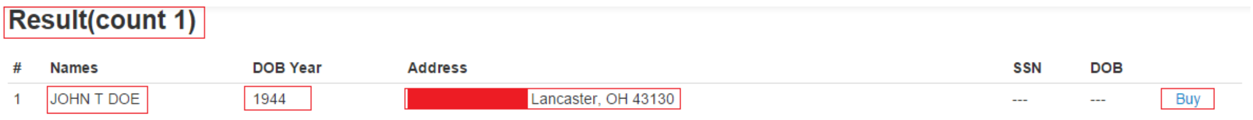
Lets look for a different John Doe again, this time from Lancaster, Ohio.



Search

First Name*:	John
Last Name*:	Doe
State*:	Ohio
City:	Lancaster
ZIP:	

You can also filter the information there as seen above, to get the most accurate results.



Result(count 1)

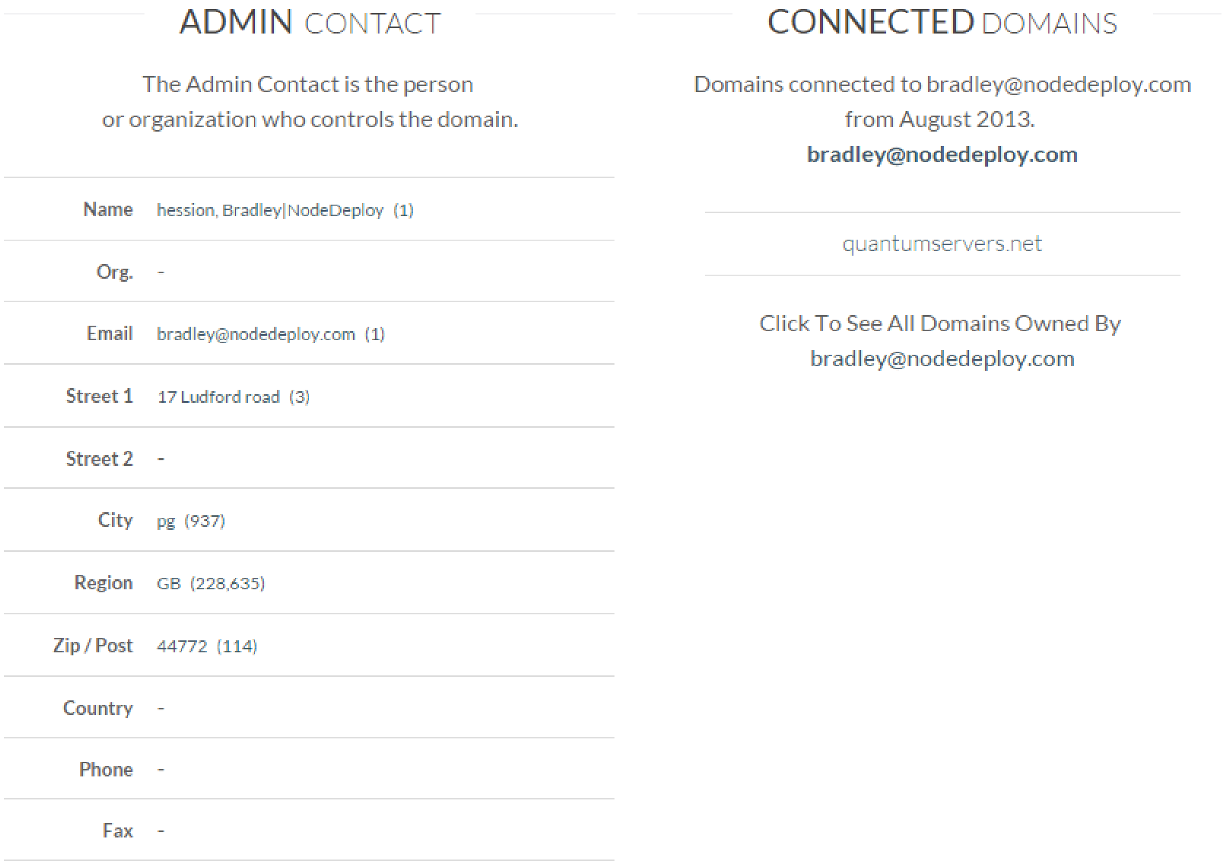
#	Names	DOB Year	Address	SSN	DOB	
1	JOHN T DOE	1944	[redacted] Lancaster, OH 43130	---	---	Buy

You need to buy credits in order to unlock the **SSN**. You can pull additional information with the SSN of the victim, for example submit the IRS for tax revenue or pull credit card reports. But we don't cover that on this eBook. This is as far as we can go without going borderline between grey and black.

1.2.7 Web & Network Forensics: WhoIs Look-Up (*Whoisology*)

Sometimes people forgot to buy WhoIs protection when they buy a domain (or just don't want to pay for it). For that reason we have tools that can exploit that lack of security from those who are lazy or don't want to afford domain protection. That's where whoisology.com comes in. You type in the domain name and it retrieves results. And hopefully, they won't be WhoIs protected.

Lets search for the owner of quantumservers.net there.



ADMIN CONTACT

The Admin Contact is the person
or organization who controls the domain.

Name	hession, Bradley|NodeDeploy (1)
Org.	-
Email	bradley@nodedeploy.com (1)
Street 1	17 Ludford road (3)
Street 2	-
City	pg (937)
Region	GB (228,635)
Zip / Post	44772 (114)
Country	-
Phone	-
Fax	-

CONNECTED DOMAINS

Domains connected to bradley@nodedeploy.com
from August 2013.
bradley@nodedeploy.com

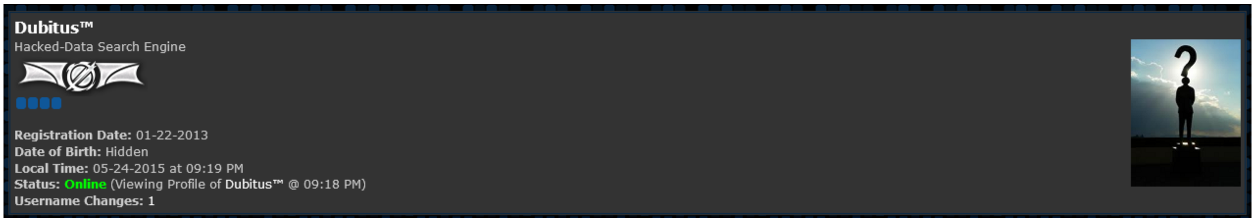
quantumservers.net

Click To See All Domains Owned By
bradley@nodedeploy.com

It's pretty much self-explanatory. Easy way to find additional information.

1.2.8 Web & Network Forensics: Reverse Image

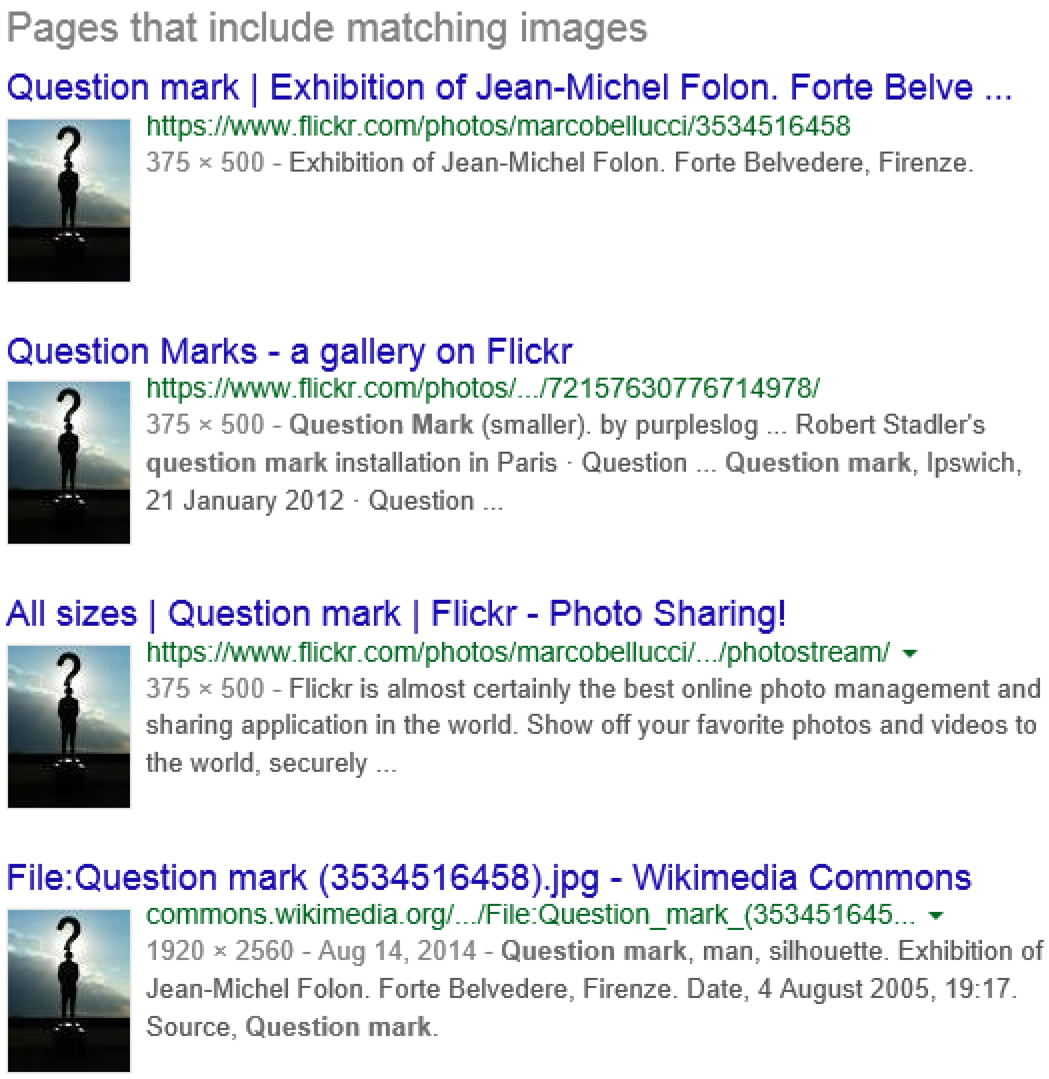
Reverse Image is the act of reversing an image to find results. Lets take my profile image on Hackforums.net for example. It's the image on the **Right**.



Dubitus™
Hacked-Data Search Engine

Registration Date: 01-22-2013
Date of Birth: Hidden
Local Time: 05-24-2015 at 09:19 PM
Status: **Online** (Viewing Profile of **Dubitus™** @ 09:18 PM)
Username Changes: 1

We copy that image, and now we head to Google and click on "**images**" and "**search by images**".



Pages that include matching images

Question mark | Exhibition of Jean-Michel Folon. Forte Belve ...
https://www.flickr.com/photos/marcobellucci/3534516458
375 × 500 - Exhibition of Jean-Michel Folon. Forte Belvedere, Firenze.

Question Marks - a gallery on Flickr
https://www.flickr.com/photos/.../72157630776714978/
375 × 500 - **Question Mark** (smaller). by purpleslog ... Robert Stadler's **question mark** installation in Paris · Question ... **Question mark**, Ipswich, 21 January 2012 · Question ...

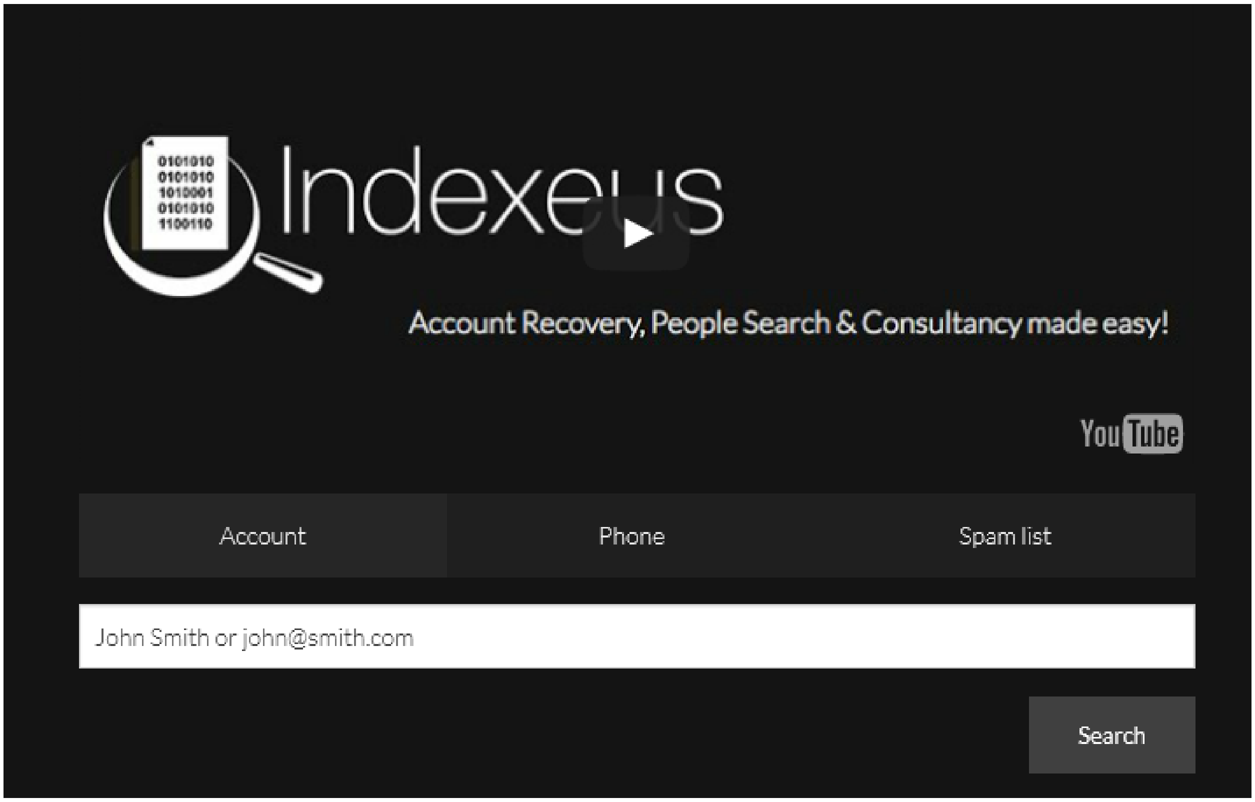
All sizes | Question mark | Flickr - Photo Sharing!
https://www.flickr.com/photos/marcobellucci/.../photostream/ ▾
375 × 500 - Flickr is almost certainly the best online photo management and sharing application in the world. Show off your favorite photos and videos to the world, securely ...

File:Question mark (3534516458).jpg - Wikimedia Commons
commons.wikimedia.org/.../File:Question_mark_(353451645... ▾
1920 × 2560 - Aug 14, 2014 - **Question mark**, man, silhouette. Exhibition of Jean-Michel Folon. Forte Belvedere, Firenze. Date, 4 August 2005, 19:17. Source, **Question mark**.

From there we can potentially find new aliases from people that uploaded that image or are using it themselves. You can also do that with photos to identify fake identities or legitimate ones.

1.2.9 Web & Network Forensics: Hacked-Data Search Engine

Hacked-Data Search Engine was a term coined by me (**Dubitus**) and **ManDoR** when we first launched indexeus.com . It’s the first of its kind, on a whole new niche under the Data-Mining Search Engine.



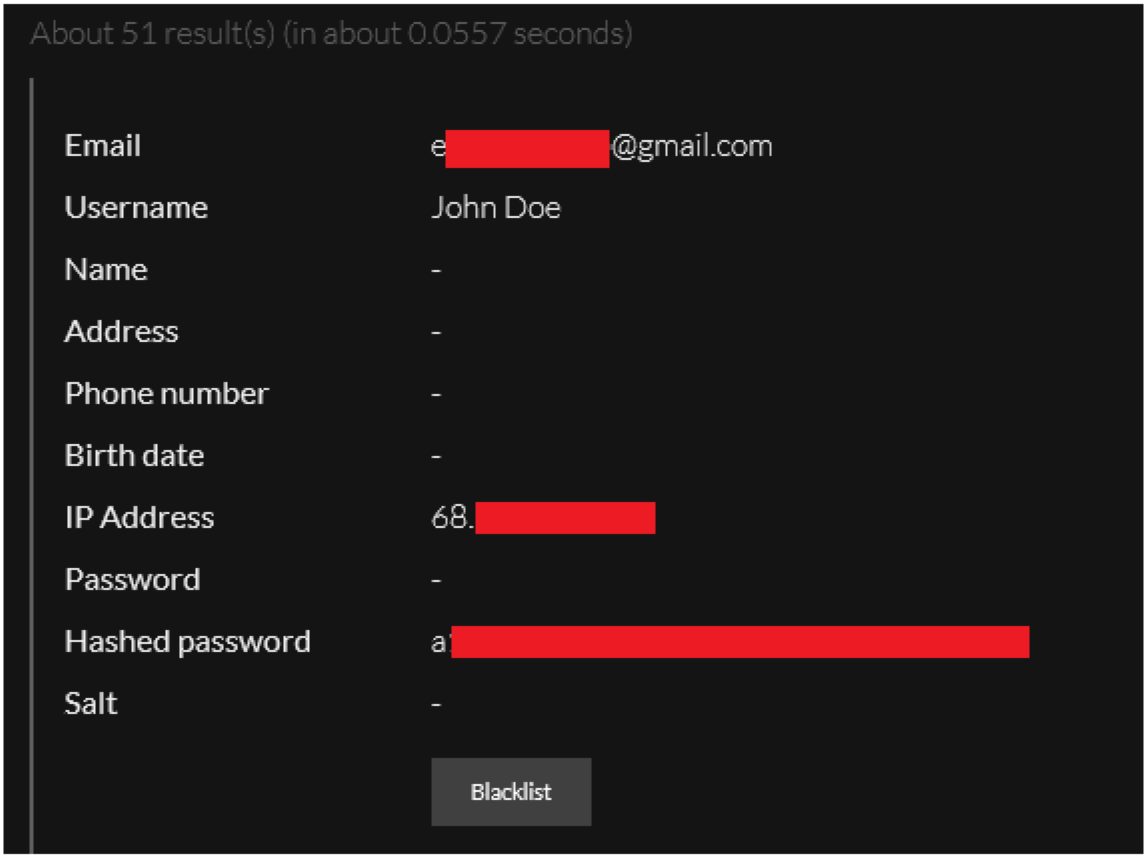
Indexeus
Account Recovery, People Search & Consultancy made easy!
YouTube
Account
Phone
Spam list
John Smith or john@smith.com
Search

Presentation Video: https://www.youtube.com/watch?v=hOK-UdUf6qo

Indexeus is a free hacked-data search engine, a revolutionary account security & consultancy tool to retrieve accounts from hacked databases that have been made public on the internet.

You never know when you've been exposed, so Indexeus will provide you with the necessary instructions and guidance to facilitate access and consultancy of such information.

You can search for a name, nickname, email, phone number, IP and address. We are not only a hacked-data search engine, but we also act as a people search and spam list search. It's everything in a little box.



About 51 result(s) (in about 0.0557 seconds)

Email	e[redacted]@gmail.com
Username	John Doe
Name	-
Address	-
Phone number	-
Birth date	-
IP Address	68.[redacted]
Password	-
Hashed password	a[redacted]
Salt	-

You can use Indexeus by inserting your search term on our search bar. It can be a username, name, email address, phone number and even an IP. And upon registration, we'll retrieve the results of your searching term, if existing. it's completely free to use. All you need to do is search for your term, then register, and retrieve the information from our system. It's a completely free account consultancy system.

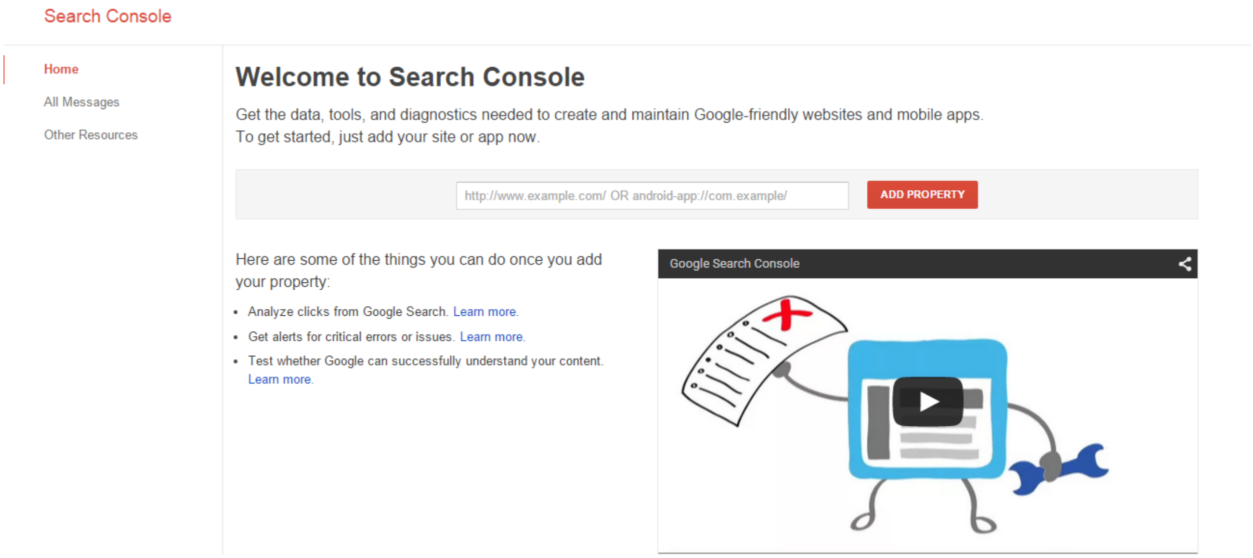
If your information is on Indexeus, you can send us a message (visit the Contact Page) to know where your information came from, and how can you remove it. We'll also give you some tips on the Help Desk to help you better secure your information and accounts.

Chapter Two

2.1 - Anti-Computer Forensics: Deindexation

The first thing about anti-computer forensics, is knowing how to properly remove leaked or exposed information from a basic web browser search engine. The process of doing this, is known as “Deindexation”, which is defined as, “to remove from an index or any system of indexing, and to no longer be index-linked”.

There are many ways you can go about performing deindexation, obviously a common way to do this is to simply report a post to Google’s Webmaster page, and the link along with it’s cache can be wiped completely from the search engine.



Welcome to Search Console

Get the data, tools, and diagnostics needed to create and maintain Google-friendly websites and mobile apps.
To get started, just add your site or app now.

Here are some of the things you can do once you add your property:

- Analyze clicks from Google Search. Learn more.
- Get alerts for critical errors or issues. Learn more.
- Test whether Google can successfully understand your content. Learn more.

However, I personally have labelled and developed and even invented 12 personal and private methods that I use solely for the purpose of deindexation, I will now share them with you. Leaking of these will result in me personally destroying your life, if you don’t believe me, test me.

2.1.1 - Ego’s Private Methods: Cloaking

Cloaking is the act of essentially copying the contents of a page, and then creating alterations to the content to benefit your online identity and to mask information that could have already possibly been leaked. In short, you are simply copying information that has already been released and then making **slight** alterations to this original content and then posting it as an updated version. The top sites to perform this on are:

1) pastebin.com
2) skidpaste.org
3) ghostbin.com
4) fbi.yt

5) weebly.com > this is for website alterations or domain redirecting (will be discussed later)

You may be asking, how this can possibly assist me if I am essentially reposting legit information on myself? Well, the answer to this question is that yes you are posting legit information on yourself or a client, but if you are making alterations, you are giving the illusion that you are updating the dox. If you continue this method over the timespan of roughly 3-5 days, you will have redirected most if not all searches for the original dox, to your own fake dox with complete alterations, making it now look like the legit and updated dox on you or your client.

2.1.2 - Ego's Private Methods: Cloned Content

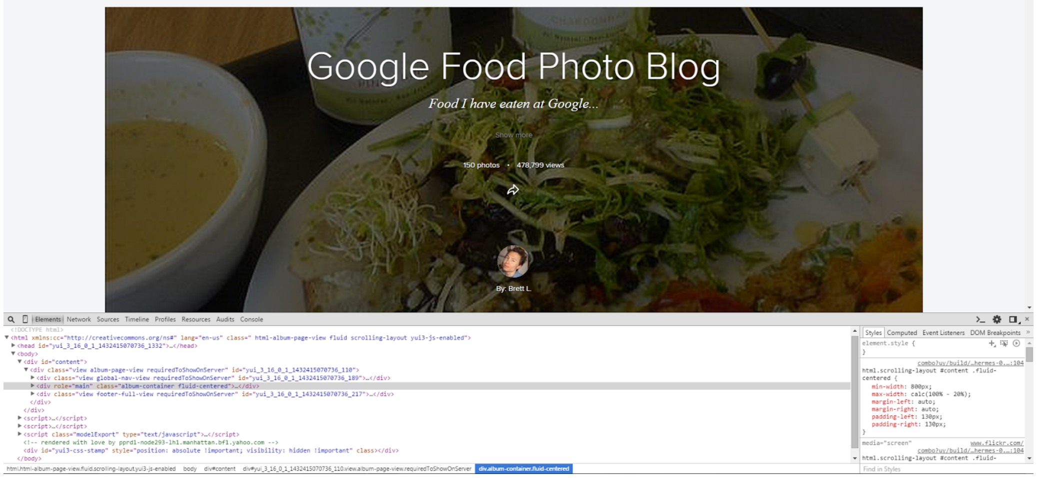
Extremely similar to cloaking, however instead of a single page, you are pasting the same information multiple times usually more than 20 times. Another thing to take note of, is that google uses the "tag" system when ranking pages submitted by SEO's. This tagging system can be exploited by using the google search operators demonstrated in chapter 1. Specifically, in chronological order and order you should place them in the search bar:

1) "site:the site you're copying goes here" (e.g. "site:hackforums.net")
2) "cache:the keywords you want to convey go here" (e.g. "cache:The Doxing Bible")
3) the use of the "#", as this makes it trending for social media applications that are using the search engine on their mobile phones or browsers.

The reason behind posting it multiple times is, again, alternating the page ranking of the original post (e.g. your dox or a client's dox), to respectively reverse which dox appears first in google search results, either your faked and alternated dox, or the original dox. By making your fake dox appear first when searching for these "tags" that you've implemented, you are creating a form of trail obfuscation and are essentially leading your pursuer into a dead end. This is the exact action you want to lead them in.

2.1.3 - Ego's Private Methods: Slaved Content

Slaved content is the act of having people formulate the keywords (tags) for you. Essentially, you are able to grab the inspect element coding for a web page and alter the code in your favour before posting it on one of the sites mentioned before. This will redirect searches (such as sites with your Skype name on them) to your post, and depending on your "pages" ranking, they may see it before the actual page itself. For Example:



```
<!DOCTYPE html>
▼<html xmlns:cc="http://creativecommons.org/ns#" lang="en-us" class=" html-album-page-view fluid scrolling-layout yui3-js-enabled">
 ▶<head id="yui_3_16_0_1_1432415070736_1332">…</head>
 ▼<body>
  ▼<div id="content">
   ▼<div class="view album-page-view requiredToShowOnServer" id="yui_3_16_0_1_1432415070736_110">
    ▶<div class="view global-nav-view requiredToShowOnServer" id="yui_3_16_0_1_1432415070736_189">…</div>
    ▶<div role="main" class="album-container fluid-centered">…</div>
    ▶<div class="view footer-full-view requiredToShowOnServer" id="yui_3_16_0_1_1432415070736_217">…</div>
    </div>
   </div>
  ▶<script>…</script>
  ▶<script>…</script>
  ▶<script class="modelExport" type="text/javascript">…</script>
   <!-- rendered with love by pprd1-node293-lh1.manhattan.bf1.yahoo.com -->
   <div id="yui3-css-stamp" style="position: absolute !important; visibility: hidden !important" class></div>
  </body>
```

```
html.html-album-page-view.fluid.scrolling-layout.yui3-js-enabled  body  div#content  div#yui_3_16_0_1_1432415070736_110.view.album-page-view.requiredToShowOnServer  div.album-container.fluid-centered
```

```
element.style {
}
                              combo?uy/build/…hermes-0.…:104
html.scrolling-layout #content .fluid-
centered {
   min-width: 800px;
   max-width: calc(100% - 20%);
   margin-left: auto;
   margin-right: auto;
   padding-left: 130px;
   padding-right: 130px;
}
media="screen"                              www.flickr.com/
                              combo?uy/build/…hermes-0.…:104
html.scrolling-layout #content .fluid-
```

As seen in the example above, I am grabbing the inspect element coding from a common site, this one happens to be a Google Food Photo Blog. Upon grabbing the coding from the site, I can copy and paste it into the sites mentioned early, to then automatically increase the page ranking for your fake dox or keywords, due to Google's hidden page ranking system, which acts as a giant scanner. If this scanner detects things that have been deemed by Google to be already published, coded, paid for (advertisements), or are low quality… the page ranking will alter accordingly. This is an extremely important concept to grasp when dealing with Footprint removal, as it has a significant impact on how fast or for how long the real information will be covered or hidden compared to the fake content you are producing.

2.1.4 - Ego's Private Methods: Keyword Scrambling

Keyword scrambling is essentially altering the keywords that people would search for when looking for your information and then placing false leads based on this already leaked information. As you now know, through the use of Google Search Operators, there are many ways that you are able to search for a variety of information/data that can be presented to you on the web. You are able to exploit these search operators to enhance the chance of your fake information to be displayed on the first search page when users use the keywords that you implemented. Obviously these keywords will change depending on the task at hand, but it is important to note that you want to link your keywords for the fake information and relate them to the original contents or link them to further false leads. An example of this in simplest form would be the following:

If someone searches "Tokyo Dox", the result is the 4th result down. Key words for this search would be "Tokyo" and "Dox".

However once they see the dox that is already existing, they will gain access to a skype name, which is: s7_vexx < This can now become a new keyword to be used to link to more false information. If you were now to search: "s7_vexx", a whole new alias would open up as well as linking to further data, which is driving your pursuer further and further away.

This is the most simple form of de-tracement, as it is basically text altercation but with added fake information, this will be discussed more in depth when we get to data poisoning.

2.1.5 - Ego’s Private Methods: Altercation of Page Ranking

Page ranking altercation occurs when you post low quality sites and affiliate them with your already leaked information. By doing so, you will drag all information that is posted at high ranking google pages down, as this exploits the tag system implemented by google SEO’s. This is an extremely easy yet effective method of de-tracing, some sites that I recommend are normally affiliated with Google Dorks:

https://www.exploit-db.com/google-hacking-database/13/
https://www.exploit-db.com/google-hacking-database/10/
https://www.exploit-db.com/google-hacking-database/14/

Just keep in mind that you want to link these within the dox to make them blend in, or simply post them at the bottom to keep them out of the way of the false information that you’ve placed. This method is extremely effective when used properly, so master it!

2.1.6 - Ego’s Private Methods: Font Matching

Font matching occurs when you match the font of a page with font that you can alter in a word document. Normally you are able to search the font used on a certain site if you are unsure, but common ones are:

1) Open Sans
2) Arial
3) Typewriter
4) Times New Roman

You then take an image of this font, with a PNG background (used via photoshop/gimp), and are able to post it on forums and such to make it look like the site is saying something other than what it intends. This normally is the hardest de-indexation method, as it normally involves XSS (Cross Site Scripting) hacking to apply an image within the code of a website to make it look as though it belongs there. I would not recommend performing this method if you are not good with XSS hacking, also, most sites that information is leaked on involves tight security and will not be vulnerable to XSS hacking, therefore you need to find sites that are and implement this method through those sites only.

2.1.7 - Ego’s Private Methods: Infoscoping

Personally coined by myself, this term refers to positing font that is essentially microscopic to the naked eye, but is still cached by google’s index and can be seen via the description under hyperlinks when the search results are visible. By performing this method, you can place words on a completely irrelevant paste, and it will confused anyone trying to gain access to your information. It is an extremely cunning method, which I use personally, and it is extremely effective.

However for sites that have case sensitive posting privileges/restrictions, use the following firefox add-on/extension to bypass case sensitive security features:

1. Go to about:config
2. Search for dom.event.clipboardevents.enabled
3. Double-click it to change the value to "false"

Use the keyword scrambling method to ensure successful results with this method, for example if you were to use the same keywords that were implemented before and apply them to this method; when someone searches for the keywords, they will cache as normal font size (via the description) and will be microscopic when the pursuer clicks the hyperlink and sees the content of the page, which can be a completely fake and non-related dox or piece of information.

2.1.8 - Ego's Private Methods: Doorway Pages

Doorway pages is a common SEO term which refers to posting links which appear to be affiliated with the original content of a page, only to be a trap door and unleashes a whole new spectrum of fake information on your pursuer. Also closely linked with data poisoning and data obfuscation, which will be discussed in a moment. An example of this would be posting legit information on yourself, and redirecting them to another link which appears to affiliate but really drives them further away.

You are able to create a long chain of doxes that can link to one another and appear to being "updated", if you are not getting what I am trying to iterate towards you, please look at this example carefully:

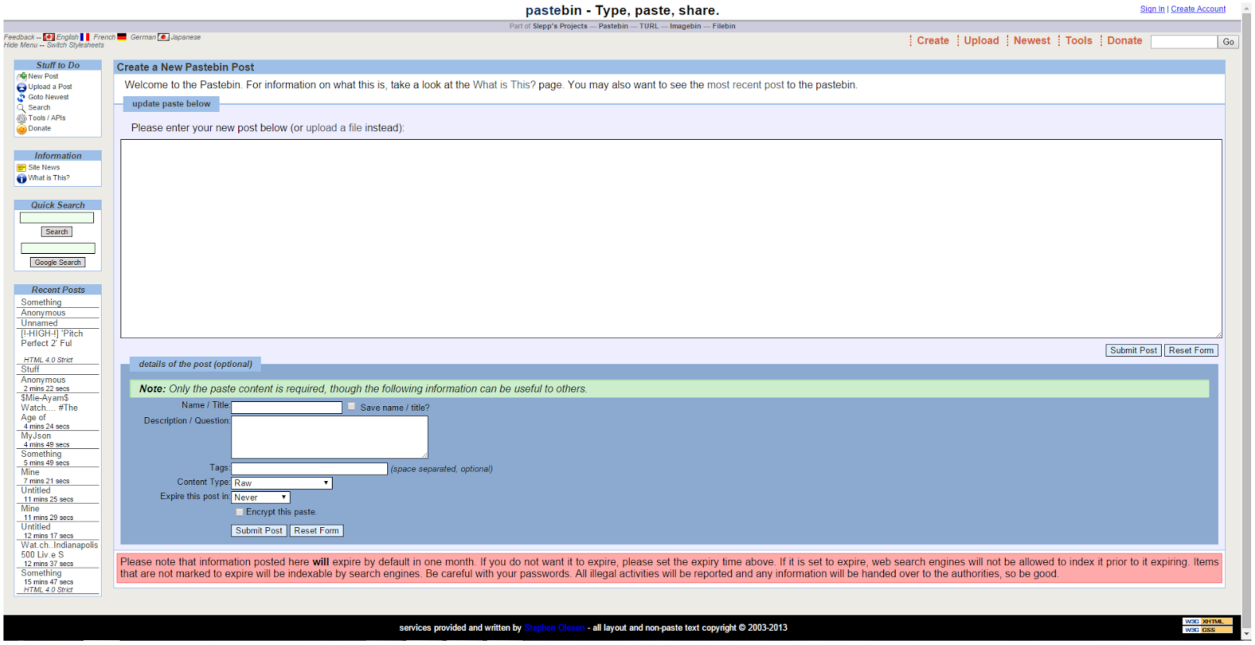
If you plan to establish a false lead using this method, you need to have a select date in which the trail will be formed. For example if the date is, 01/15/2015 and we want to use the date, 01/01/2015, and state that this is the date we want the trail to start on, we need to create a false dox for this specific date. Once you have created this fake dox, you need to make a new paste on one of the sites mentioned earlier, with the title: "Dox on" "Target name here" "updated" "insert the selective date here, in this case it would be 01/01/2015". Although the date you publish this post will be listed as 01/15/2015, it will go unnoticed by a common pursuer and they will think it's posted on the date you stated in the title.

You then repeat your this step over the following 14 days proceeding up to the 15th (or the date you set the trail to end), and always keep linking the url to the previous dox post to ensure there is a connection between the doxes. By doing this you can make a massive trail and the date will be continues to appear as those it's being updated.

2.1.9 - Ego's Private Methods: The 100:1 Principle

The 100 to 1 principle is defined as a method to essentially spam false information to most places on the web, and by doing so, you will make false information appear far more legitimate. The use of iMacros (firefox and google chrome extension), allows you to record actions you are performing within your search browser, creating a "macro" and you can repeat this macro as many times as you like, although you are not the one actually performing the actions, it’s iMacros. There are however certain sites this works best on, sites that **do not** have ip restrictions or captcha security settings cannot be used, as they block spamming. The following sites are my top two for performing this method:

1) http://pastebin.ca
2) http://slexy.org



pastebin - Type, paste, share.

Create a New Pastebin Post

Welcome to the Pastebin. For information on what this is, take a look at the What is This? page. You may also want to see the most recent post to the pastebin.

Please enter your new post below (or upload a file instead):

Note: *Only the paste content is required, though the following information can be useful to others.*

Name / Title: ☐ Save name / title?

Description / Question:

Tags: *(space separated, optional)*

Content Type: Raw

Expire this post in: Never

☐ Encrypt this paste.

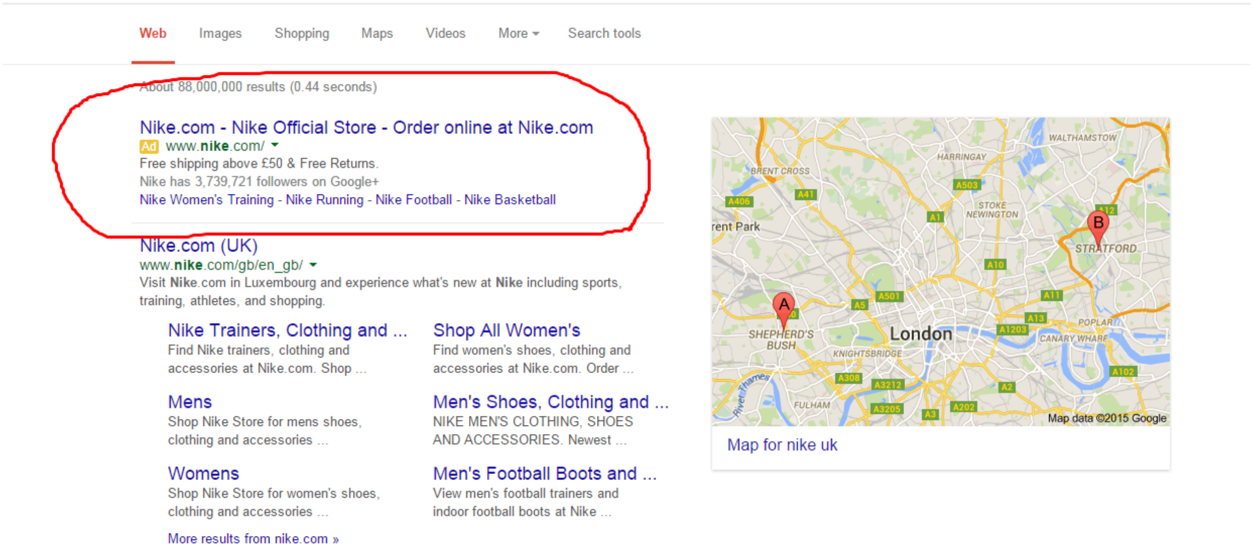
Please note that information posted here **will** expire by default in one month. If you do not want it to expire, please set the expiry time above. If it is set to expire, web search engines will not be allowed to index it prior to it expiring. Items that are not marked to expire will be indexable by search engines. Be careful with your passwords. All illegal activities will be reported and any information will be handed over to the authorities, so be good.

services provided and written by Stephen Olesen - all layout and non-paste text copyright © 2003-2013

You then record the script, in this case it would be the contents of a fake dox, and then play the script a few times and you can instantly get 1500 searches within a matter of minutes. This will not only increase the page ranking of you fake information, but will also make the contents seem far more reliable and believable.

2.1.10 - Ego’s Private Methods: Rich Snippets

Rich snippets are essentially an SEO term for advertisements on google. You may see an ad for Mary’s Golden Dildos or something of that nature when you search for a song on google, and this is a perfect example of a rich snippet.



About 88,000,000 results (0.44 seconds)

Nike.com - Nike Official Store - Order online at Nike.com
Ad www.nike.com/
Free shipping above £50 & Free Returns.
Nike has 3,739,721 followers on Google+
Nike Women's Training - Nike Running - Nike Football - Nike Basketball

Nike.com (UK)
www.nike.com/gb/en_gb/
Visit Nike.com in Luxembourg and experience what's new at Nike including sports, training, athletes, and shopping.

Nike Trainers, Clothing and ...
Find Nike trainers, clothing and accessories at Nike.com. Shop ...

Shop All Women's
Find women's shoes, clothing and accessories at Nike.com. Order ...

Mens
Shop Nike Store for mens shoes, clothing and accessories ...

Men's Shoes, Clothing and ...
NIKE MEN'S CLOTHING, SHOES AND ACCESSORIES. Newest ...

Womens
Shop Nike Store for women's shoes, clothing and accessories ...

Men's Football Boots and ...
View men's football trainers and indoor football boots at Nike ...

More results from nike.com »

However these rich snippets can be exploited, by you simply copy and paste the rich snippet URL to a paste site, and it will automatically bump it up in the google page ranking system. Why? Well as stated before, if you were to think of Google or any search engine for that matter, as a giant scanner, that scans your contents word for word, you can come to realise that Google Processes page ranking and keywords and search results based on what it scans. By implementing a rich snippet URL, you are letting Google scan your page, and say “hey, this is registered as a URL to a paid advertisement, this needs to have higher page ranking”, which is essentially what it will do. Now granted, this will not automatically bump your post to the front page, however it will bump it up quite considerably.

An issue with these page snippets however need to be constantly updated, as google’s page snippets update almost daily. So long as you do that, you will be fine in terms of keeping your dox at a constant higher page ranking.

2.1.11 - Ego’s Private Methods: Site Duplication

This is a combination of Doorway Pages and the 100 to 1 Principle. You essentially create a competing dox that has been release of you, use the iMacros technique while in the mean time altering the information slightly on your original dox, and your main aim is to outrank the site that currently has your dox released. Again altering the page rankings. This method is really not that hard to grasp and is quite possibly one of the most effective as it is utilising two methods into one and making a greater impact. If you do not understand this method for whatever reason, please contact me.

2.1.12 - Ego’s Private Methods: Interlinking

This is a basic scheme that takes advantage of the importance of inbound links in search engine ranking by building dozens of sites and then linking them to each other. This can be applied to sites such as: www.pastebin.com, www.skidpaste.org, and www.weebly.com, all of which you can link false doxes to one another to make them appear as though they are being constantly updated by someone who truly dislikes you with a burning passion.

A way to do this, in a simplified example, is by doing the following:

1) Go to Pastebin.com
2) Implement your fake dox, or fake content, whatever it may be, into the “new text” section
3) Then, at the bottom after you have completely put in the fake content that you require, open a new pastebin with a link to another fake dox you have created, copy this link and paste it into the original pastebin you opened.
4) Repeat this step for roughly 5+ fake doxes you have released, make sure to include a link to another fake dox at the bottom. This will link all the pastes together in Google’s search system, one will relate to the other, even if the content is completely different.

This is an extremely good method to have a long line of false trails, while at the same time linking and compiling more and more information on top of each other for anyone that may be trying to get information on you. This is a fantastic method, even if it may be simple, it’s extremely effective.

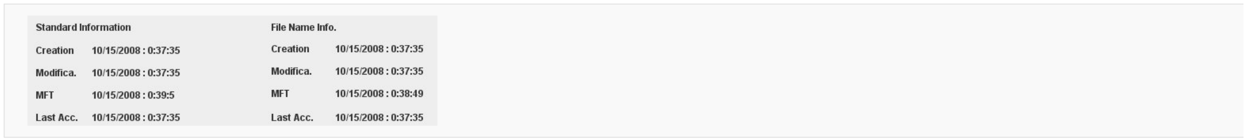
2.2 - Anti-Computer Forensics: Trail Obfuscation

The purpose of trail obfuscation is to confuse, mislead and alter someone’s perception of identity or what they are representing. There are many techniques and tools that can be used for trail obfuscation, all of which you can learn about by a simple Google search. However, the main techniques and tools that we will be looking at in-depth are going to be; TimeStomp, Transmogrify, and Data Poisoning.

2.2.1 - Trail Obfuscation: TimeStomp

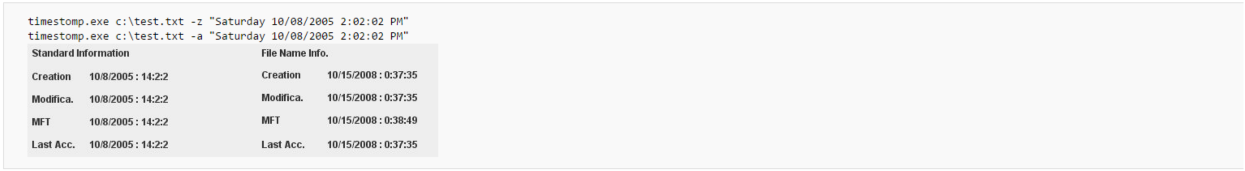
TimeStomp is an application that allows you to alter the timestamp and date in which a file was created. You are able to modify the date as well as change the timestamp completely, which is useful when trying to hide when you were looking at certain files or were editing, publishing, posting files. As a visual aid, we will use the images from Google!

1) Create file (*c:\test.txt*)



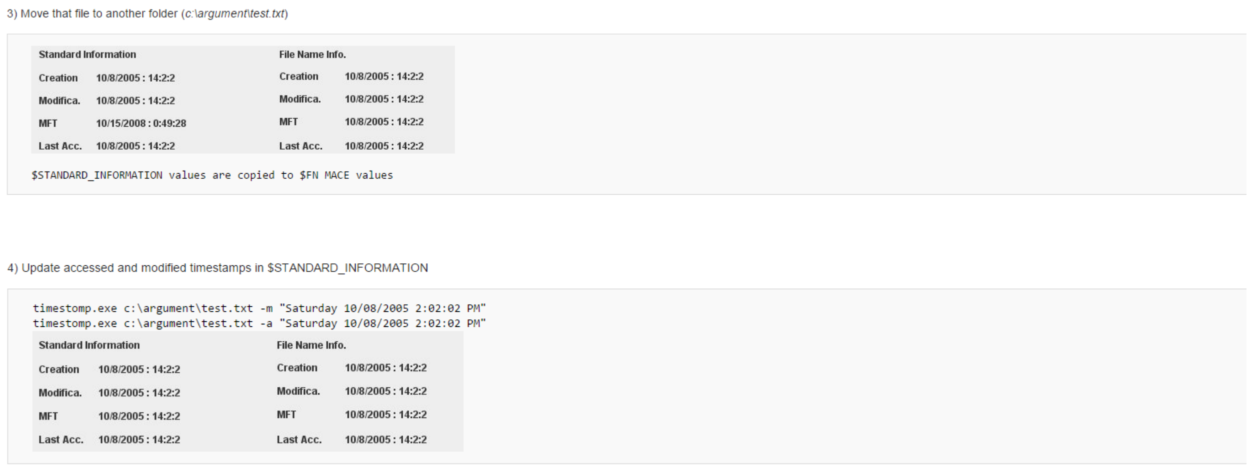
Standard Information		File Name Info.	
Creation	10/15/2008 : 0:37:35	Creation	10/15/2008 : 0:37:35
Modifica.	10/15/2008 : 0:37:35	Modifica.	10/15/2008 : 0:37:35
MFT	10/15/2008 : 0:39:5	MFT	10/15/2008 : 0:38:49
Last Acc.	10/15/2008 : 0:37:35	Last Acc.	10/15/2008 : 0:37:35

2) Change timestamps using Timestomp



```
timestomp.exe c:\test.txt -z "Saturday 10/08/2005 2:02:02 PM"
timestomp.exe c:\test.txt -a "Saturday 10/08/2005 2:02:02 PM"
```

Standard Information		File Name Info.	
Creation	10/8/2005 : 14:2:2	Creation	10/15/2008 : 0:37:35
Modifica.	10/8/2005 : 14:2:2	Modifica.	10/15/2008 : 0:37:35
MFT	10/8/2005 : 14:2:2	MFT	10/15/2008 : 0:38:49
Last Acc.	10/8/2005 : 14:2:2	Last Acc.	10/15/2008 : 0:37:35



3) Move that file to another folder (*c:\argument\test.txt*)

Standard Information		File Name Info.	
Creation	10/8/2005 : 14:2:2	Creation	10/8/2005 : 14:2:2
Modifica.	10/8/2005 : 14:2:2	Modifica.	10/8/2005 : 14:2:2
MFT	10/15/2008 : 0:49:28	MFT	10/8/2005 : 14:2:2
Last Acc.	10/8/2005 : 14:2:2	Last Acc.	10/8/2005 : 14:2:2

```
$STANDARD_INFORMATION values are copied to $FN MACE values
```

4) Update accessed and modified timestamps in $STANDARD_INFORMATION

```
timestomp.exe c:\argument\test.txt -m "Saturday 10/08/2005 2:02:02 PM"
timestomp.exe c:\argument\test.txt -a "Saturday 10/08/2005 2:02:02 PM"
```

Standard Information		File Name Info.	
Creation	10/8/2005 : 14:2:2	Creation	10/8/2005 : 14:2:2
Modifica.	10/8/2005 : 14:2:2	Modifica.	10/8/2005 : 14:2:2
MFT	10/8/2005 : 14:2:2	MFT	10/8/2005 : 14:2:2
Last Acc.	10/8/2005 : 14:2:2	Last Acc.	10/8/2005 : 14:2:2

2.2.2 - Trail Obfuscation: Transmogrify

The easiest way to perform this technique is to modify the header of a file, so that it can no longer be associated with any type of file already known to a system. Following the general structure of a Windows PE executable file for example, it always starts with a word value shown below:

HEX -> \X4D\X5A / ASCII -> MZ

Many forensic tools for recovering files within the analysed systems refer to these parameters, sometimes only the header and others both headers and footers. By changing these values, and restoring them only in case of necessity, it is possible to avoid detection of a hypothetical compromising document. This approach is adopted by "*Transmogrify,*" an anti-forensic tool. The technique basically aims to deceive the signature-based scan engine of these tools.

2.2.3 - Trail Obfuscation: Data Poisoning

Data Poisoning is a term coined by The Black Hand's very own member, Melty. This term refers to, "The act of leaving a false trail that misdirects or misleads to a different individual or trail."

Example: Alias Leaching

Alias leaching is the term of hijacking an alias, there are various levels of alias leaching, alias leaching is most successful when a person is able to hijack an email, and then grow a synthetic alias from there. Data poisoning may also include the faking or misleading of an IP address geo location, based on the research done on the previous alias, such as the original owners geographical location. Essentially you are using previous data that you have hijacked, and implementing it into present day data on an alias you may be going under or a client may want to be going under.

2.3 Anti-Computer Forensics: Data Hiding

Data hiding is an extremely simple concept, and there is not much to be discussed on it, however there are some things that you need to know to ensure that you are hiding data correctly. Data can be hidden in unallocated locations which are normally ignored or skipped over when dealing with being tested by forensic tools. The way you are able to do this is to store data in the following locations:

1) Host Protected Area (HPA)
2) Device Configuration Overlay (DCO)

These two areas are linked with areas of a modern ATA hard drive. Data that is in either the HPA or DCO are not visible to BIOS and operating systems. There are also three main sub categories when dealing with Data Hiding, they are; Encryption, Steganography, and Slacker.

2.3.1 Data Hiding: Encryption

Encryption and overall encrypted data is essential for hidden important information and making it almost impossible to be traced through the use of forensic tools. What encryption does is essentially make the information that is saved to your hard disk transparent, and is only solidified (as in readable), once it is opened again and decrypted. Although there are forensic investigators that can decrypt most cryptography, if the form of cryptography that you use on your system is unknown to the investigator, you are almost guaranteed a solid barrier when dealing with whether or not your information gets leaked.

Microsoft Word can be configured to encrypt the contents of a document by specifying that the document has a “password to open.” Another form of this is to save the file in notepad or some other basic documentation application as a .batch file, which requires passwords to see the content inside. Although older versions of Microsoft Word encrypted documents with a 40-bit key that can be cracked with commercial tools, modern versions can optionally use a 128-bit encryption that is uncrackable if a secure passphrase is used. This is highly recommended for most documents, if you are worried that they are unsecure or that you need to hide sensitive information such as passwords, login details, etc.

2.3.2 Data Hiding: Steganography

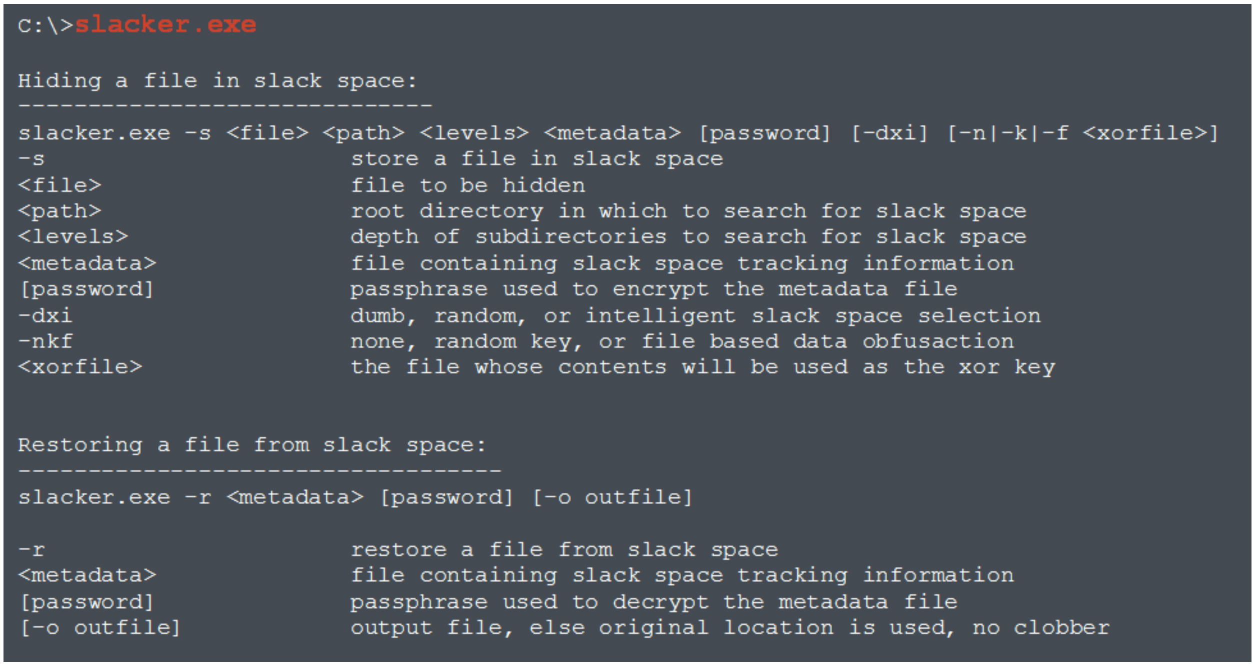
Steganography can be used to embed encrypted data in a cover text to avoid detection. This means that you are able to hide text in the format of MP3, JPEG, AVI, etc. By hiding this information within media files or non-text based files, it would make it extremely unlikely for any investigator to check these particular files. There is a program for this, it is known as the following:

StegFS (Download Link: http://sourceforge.net/projects/stegfs/)

What StegFS does is “hides encrypted data in the unused blocks of a Linux ext2 file system, making the data “look like a partition in which unused blocks have recently been overwritten with random bytes using some disk wiping tool”. - (McDonald and Kuhn, 2003)

2.3.3 Data Hiding: Other Forms of Data Hiding (Slacker)

Slacker is a commonly used data hiding forensic tool, and it is used via your command prompt, as is TimeStomp, which was mentioned earlier. “Slacker allows you to hide data in the slack space of NTFS. This slack space is created when a file system allocates space for a file to be written, it will typically allocate more space than it actually uses. The unused space is called slack space and perfect data-hiding grounds for the hacker.” - Slacker’s official website.



```
C:\>slacker.exe

Hiding a file in slack space:
------------------------------
slacker.exe -s <file> <path> <levels> <metadata> [password] [-dxi] [-n|-k|-f <xorfile>]
-s                        store a file in slack space
<file>                    file to be hidden
<path>                    root directory in which to search for slack space
<levels>                  depth of subdirectories to search for slack space
<metadata>                file containing slack space tracking information
[password]                passphrase used to encrypt the metadata file
-dxi                      dumb, random, or intelligent slack space selection
-nkf                      none, random key, or file based data obfusaction
<xorfile>                 the file whose contents will be used as the xor key


Restoring a file from slack space:
-----------------------------------
slacker.exe -r <metadata> [password] [-o outfile]

-r                        restore a file from slack space
<metadata>                file containing slack space tracking information
[password]                passphrase used to decrypt the metadata file
[-o outfile]              output file, else original location is used, no clobber
```

2.4 Anti-Computer Forensics: Artifact Wiping

Artifact wiping methods are tasked with permanently removing particular files or entire file systems. There are three core principles to artifact wiping, which will be displayed as core sub-categories of this terminology; Disk Cleaning Utilities, File Wiping Utilities, Disk Degaussing and Destruction Techniques.

2.4.1 Artifact Wiping: Disk Cleaning Utilities

Disk cleaning utilities are extremely essential for artifact wiping as the essentially overwrite existing data on the disks of your computer. There are many arguments that go against this method, and claim that disk cleaning utilities are not actually cleaning anything, as they are leaving fingerprints of what has been removed and when or where it was removed from. Some very useful programs for disk cleaning will be linked below:

1) http://www.jetico.com/products/personal-privacy/bcwipe/
2) http://www.r-wipe.com/
3) http://www.aevita.com/file/delete/
4) http://www.cyberscrub.com/

Out of all of these, I personally would highly recommend either BCwipe or cyberscrub. These have probably the best reputation in terms of reviews and consistency.

2.4.2 Artifact Wiping: File Wiping Utilities

File wiping utilities are as the name suggests, they are tools used for wiping single or individual files from an operating system. These are normally much faster to remove as they are only wiping a single content source as oppose to a large string of files or an entire file system. It is because of this very reason that singular file wiping utilities have much smaller, if not non-existent, signatures within a system. They are much harder to detect, and investigators struggle to find these signatures.

Again, there are extremely similar tools to use or look into when dealing with File Wiping Utilities, but if you're looking to download less software and do twice as much cleaning on your machine, I would recommend, once again, downloading:

1) http://www.jetico.com/products/personal-privacy/bcwipe/

2.4.3 Artifact Wiping: Disk Degaussing | Destruction Techniques

Disk degaussing is the term for completely wiping and destroying the process that is your hard drive or disk drive. This is done through the use of an magnetic field being applied to your hardware, the data of this device or disk is completely wiped, meaning there is absolutely no trace. Although this is extremely expensive to had done, this is quite possibly the best and most effective method to use when wanting to hide information/data and completely wipe any trace of you ever having this information. Destruction techniques include pulverisation, disintegration, incineration, shredding and melting. Take a pick, I'm sure one will work just fine.

Contact Us

If you wish to further your knowledge of web forensics and footprint removal, we have some suggestions for you. We highly recommend

you join The Black Hand’s mentoring program, in which you will be placed into practical work after learning theory, and will be tested to possibly gain a chance to join the group on a trial basis. Another program that you can check out is Null Consolidated’s White Hat Hacking student program. You learn extremely valuable skills, not just revolving around forensic work, but you will become familiar with all aspects of hacking within a matter of months.

Dubitus Contact Information: dubitus@protonmail.ch
Ego Contact Information: himitsu@riseup.net